

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
Twenty-five (25) Google accounts owned by Google LLC.,
headquartered at 1600 Amphitheatre Way, Mountain
View, California, as further described in Attachment A.

Case No. MJ21-210

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Twenty-five (25) Google accounts owned by Google LLC., headquartered at 1600 Amphitheatre Way, Mountain View, California, as further described in Attachment A.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 1343
18 U.S.C. § 641
18 U.S.C. § 1956
18 U.S.C. § 1028A

Wire Fraud
Theft of Public Property
Money Laundering
Aggravated Identity Theft


Offense Description

The application is based on these facts:

- ☒ See Affidavit of IRS-CI Special Agent Eric Litster, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.



Applicant's signature

Eric Litster, IRS-CI Special Agent

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
- ☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 4/9/21


Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge

Printed name and title

AFFIDAVIT OF SPECIAL AGENT ERIC LITSTER

STATE OF WASHINGTON)
) SS
COUNTY OF KING)

I, Eric Litster, having been duly sworn, state as follows:

INTRODUCTION

1. I am a Special Agent with the Internal Revenue Service, Criminal Investigation (IRS-CI), stationed in Seattle, Washington, and have been so employed since approximately February 2019. My duties and responsibilities include the investigation of possible criminal violations of the Internal Revenue laws (Title 26, United States Code), the Bank Secrecy Act (Title 31, United States Code), the Money Laundering Control Act of 1986 (Title 18, United States Code, Sections 1956 and 1957), and other related offenses.

2. I earned a Bachelor of Science in accounting from Brigham Young University in 2009 and a Master of Science in taxation from Boise State University in 2010. In 2019 I graduated from the Criminal Investigator Training Program and the IRS Special Agent Basic Training at the Federal Law Enforcement Training Center (FLETC) where I received detailed training in conducting financial investigations. The training included search and seizure, the Internal Revenue laws, and IRS procedures and policies in criminal investigations. I have also attended various cybercrime and virtual currency related trainings. I have conducted and assisted in numerous investigations involving financial crimes such as tax evasion (26 U.S.C. § 7201), filing a false tax return (26 U.S.C. § 7206(1)), aiding or assisting in the preparation of false tax returns (26 U.S.C. § 7206(2)), conspiring to defraud the United States (18 U.S.C. § 371), wire and mail fraud (18 U.S.C. §§ 1343, 1341), aggravated identity theft (18 U.S.C. § 1028A), and money laundering (18 U.S.C. §§ 1956, 1957), among others. I have participated in the execution of search warrants and have interviewed witnesses and defendants who were involved in, or had knowledge of, violations of the Internal Revenue Code, the Bank Secrecy Act, and

1 the Money Laundering Control Act. Before being hired by IRS-CI, I was employed for
2 approximately six years as a project manager and a senior tax analyst for a Fortune 500
3 chemical distribution company and for approximately two years as a tax analyst at a large
4 public accounting firm in New York City. I am a Certified Public Accountant.

5 3. I am investigating a massive fraud on the Washington Employment
6 Security Department (ESD). The fraud involves the theft of hundreds of millions of
7 dollars that were intended to provide economic relief to Washington workers affected by
8 the COVID-19 pandemic. The investigation has revealed that criminals submitted
9 thousands of fraudulent unemployment claims to ESD using the stolen personal
10 identifying information of unwitting third persons. The fraudulent applications requested
11 that the benefits be paid to bank accounts and payment cards controlled by persons
12 known as "money mules," who withdrew and further dissipated the funds. The conduct
13 under investigation violated numerous federal criminal statutes, including 18 U.S.C. §
14 1343 (wire fraud), 18 U.S.C. § 641 (theft of public property), 18 U.S.C. § 1956 (money
15 laundering) and 18 U.S.C. § 1028A (aggravated identity theft).

16 4. This affidavit is submitted in support of an application to search a
17 collection of 25 email accounts hosted by Google Corporation (collectively referred to as
18 the "SUBJECT ACCOUNTS"), which are listed on Attachment A.

19 5. As discussed herein, the SUBJECT ACCOUNTS were used by the
20 perpetrator/s in the course of submitting fraudulent claims or connected to those accounts
21 submitting fraudulent claims; therefore, probable cause exists to believe that the
22 SUBJECT ACCOUNTS will contain evidence and instrumentalities of the offenses listed
23 above. The requested warrant would require Google to disclose to law enforcement the
24 material listed on Attachment B.I, and would authorize law enforcement officers to
25 search for, and seize, the material listed on Attachment B.II.

26 6. The information set forth in this affidavit is not intended to detail each and
27 every fact and circumstance of the investigation or all information known to me or the
28

1 | investigative participants. Rather, this affidavit is intended to present the facts relevant to
2 | the issue of whether probable cause exists to issue the requested search warrant.

3 | 7. This Court has jurisdiction to issue the requested warrant because it is “a
4 | court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the Court
5 | is “a district court of the United States . . . that has jurisdiction over the offense being
6 | investigated.” 18 U.S.C. § 2711(3)(A)(i).

7 |
8 | **STATEMENT OF PROBABLE CAUSE**

9 | **A. The CARES Act**

10 | 8. Based on publicly available information, I know that on March 27, 2020,
11 | the United States enacted into law the Coronavirus Aid, Relief, and Economic Security
12 | (CARES) Act. The CARES Act authorized approximately \$2 trillion in aid to American
13 | workers, families, and businesses to mitigate the economic consequences of the COVID-
14 | 19 pandemic. The CARES Act funded and authorized each state to administer new
15 | unemployment benefits. These benefits include (1) Federal Pandemic Unemployment
16 | Compensation (FPUC), which provides an additional benefit of \$600 per week per
17 | unemployed worker; (2) Pandemic Unemployment Assistance (PUA), which extends
18 | benefits to self-employed persons, independent contractors, and others; and (3) Pandemic
19 | Emergency Unemployment Assistance (PEUC), which extends benefits for an additional
20 | 13 weeks after regular unemployment benefits are exhausted. All of these programs will
21 | be referenced herein as “CARES Act benefits.” The CARES Act allows an unemployed
22 | worker to obtain back benefits retroactive to the date on which the applicant was affected
23 | by COVID 19, which, under program rules, may be as early as February 2, 2020.

24 | 9. The Washington Employment Security Department (ESD) is the
25 | component of the State of Washington responsible for administering unemployment
26 | benefits, including CARES Act benefits. Applicants apply for ESD-administered
27 | benefits using ESD’s Secure Access Washington (SAW) web portal. To submit an
28 | application, the applicant must enter his or her personal identifying information

1 (including name, date of birth, and Social Security number). ESD checks this
2 information against its database of Washington residents. If ESD confirms that the
3 information matches the personal identifying information of a person in ESD's records,
4 ESD will pay out benefits via wire (ACH) transfer to an account identified by the
5 applicant.

6 10. Prior to March 2020, before paying unemployment benefits to a worker,
7 ESD generally required the worker's employer to provide confirmation that the employee
8 had ceased working for the employer, and further, that the circumstances surrounding the
9 termination rendered the employee eligible for unemployment assistance. However, in or
10 about March 2020, as a result of changes in eligibility resulting from the CARES Act,
11 and in an effort to distribute funds as quickly as possible, ESD stopped requiring
12 employer verification before it paid claims.

13 **B. Overview of Investigation**

14 11. Beginning on around April 20, 2020, law enforcement officials began
15 receiving complaints from employers about potentially fraudulent unemployment claims.
16 The employers reported that they had received notices from ESD indicating that persons
17 still under their employ had filed unemployment claims. For example, on or about April
18 20, 2020, the Seattle Fire Department (SFD) notified the U.S. Attorney's Office for the
19 Western District of Washington that claims had been filed in the names of multiple
20 firefighters who were actively employed by SFD. SFD reported that it had interviewed
21 the firefighters, who had denied any involvement in the claims. Other employers,
22 including Microsoft Corporation, the City of Bellingham, Zulily, and Seattle Yacht Club
23 submitted similar complaints.

24 12. Roughly around that same time, numerous other agencies, including the
25 Federal Bureau of Investigation, the Social Security Administration Office of Inspector
26 General, the United States Secret Service, the Department of Labor Office of the
27 Inspector General, the United States Postal Inspection Service, and the Internal Revenue
28 Service Criminal Investigation, joined the investigation. Agents from these agencies,

1 including myself, have reviewed voluminous financial records and databases reflecting
2 the fraudulent transactions and have conducted dozens of interviews.

3 13. Beginning on or about April 21, 2020, ESD provided claims data for the
4 limited population of claims that were then known to be fraudulent. In reviewing the data,
5 it was instantly apparent that a significant portion (approximately 35%) of the known
6 fraudulent payments were made to Green Dot cards. Green Dot cards are prepaid
7 payment cards that can be purchased at retail locations such as Walgreens or Wal-Mart.
8 After the buyer purchases the Green Dot card, he or she can fund the card through ACH
9 (wire) transfers.

10 14. Green Dot was notified of the pattern of fraudulent ESD payments being
11 loaded onto Green Dot cards. Green Dot conducted research into its own data to identify
12 other instances of fraud. Through a series of conversations with Green Dot fraud
13 investigators over the next several weeks, Green Dot advised investigators that it had
14 identified in excess of \$150 million of ESD payments to Green Dot accounts that Green
15 Dot had determined to be fraudulent. The vast majority of these payments were directed
16 to Green Dot cards that had been purchased in states other than Washington, and
17 particularly states in the Southeast region of the United States. In many cases, batches of
18 cards were purchased at a single time, and then ESD benefits were loaded onto multiple
19 cards in the same batch. Further, many of the cards had received payments issued on
20 behalf of multiple beneficiaries.

21 15. One source of data in the investigation is a database produced by ESD
22 containing claims information of claims ESD believed to be fraudulent. Investigative
23 activities have confirmed that these claims in the database are indeed fraudulent.

24 16. The database contains payment information indicating that the fraudulent
25 benefit payments were made to thousands of banks around the country. Using that
26 account information, agents have interviewed dozens of persons whose bank accounts
27 received the fraud proceeds. Investigators refer to these persons as “money mules.” In
28 many or most cases, the money mules appear to be different from the persons who

1 submitted the fraudulent claims. Many of the money mules are unwitting money mules,
2 that is, they themselves are victims of romance or employment scams and are acting at
3 the direction of others. For example, the money mule may believe that the benefit
4 payment was deposited into his or her account by an online boyfriend or girlfriend, who
5 requests that the money mule withdraw the money and send it to another account. The
6 money mules typically withdraw the fraud proceeds shortly after the proceeds are
7 deposited and then transfer the money according to instructions they receive.

8 17. The total amount of fraudulent claims paid out by ESD is currently
9 unknown. However, the ESD's Commissioner, Suzi LeVine, has publicly stated that the
10 fraud loss is likely to be between \$500 million and \$650 million.

11 **C. The SUBJECT ACCOUNTS**

12 18. As discussed above, applicants apply for ESD benefits using ESD's Secure
13 Access Washington (SAW) portal. Through communication with ESD employees and
14 review of the SAW portal, investigators have learned that, when an applicant applies for
15 benefits through SAW, the applicant is required to provide an email address. After the
16 initial application is submitted, ESD sends an authentication email to the address the
17 applicant provided. To continue the application process, the user must then access the
18 email account and click on an activation link. The user may then return to the SAW
19 portal and complete the application process. By necessity, each email account associated
20 with a fraudulent claim must have been accessed, as part of the fraud, by a participant in
21 the fraud scheme.

22 19. As discussed above, ESD has provided the government with a database of
23 the claims it has identified as fraudulent. ESD's database identifies the address of the
24 email account that was used to activate each fraudulent claim. Investigators have
25 grouped these accounts by email provider and found that over 30,000 Google-hosted
26 email accounts were used to activate fraudulent ESD claims.

27 20. **ESD Fraud Proceeds Paid to Walter Bailey:** On June 4, 2020 federal
28 agents interviewed Walter Bailey after information was obtained from Connection Credit

1 Union (CCU) that showed Bailey receiving IRS and ESD funds. Bailey said, among
2 other things, that he was in communication with at last three women he considered his
3 girlfriends and was aware that he was depositing money for them to the names and
4 accounts they provided. Bailey said he would not take a cut or receive any money for
5 moving the money for his girlfriends. Bailey was also in contact with two other
6 individuals who sent him checks to print and mail. Bailey did not know the individuals
7 listed on the checks.

8 21. Bailey was not initially aware that federal income tax refunds of
9 approximately \$7,500.00 had been deposited into his bank account at CCU in the names
10 J.S., and J.G.S. When Bailey asked one of his girlfriends about the deposits, he was told
11 that it's fine because the money was owed to them.

12 22. Bailey was also not aware that ESD payments had been directed to his bank
13 account. He did not apply for any unemployment benefits for himself or anyone else.
14 Between May 6, 2020 and May 14, 2020, six distinct ESD UI payments totaling
15 \$44,896.00 for claimants E.H, H.A.K, K.G, D.B, C.S and D.A were attempted to be
16 deposited into Bailey's bank account. CCU returned all of these ACH deposits as
17 "Account Does Not Exist."

18 23. Bailey was told by one of his girlfriends that money was owed to her from
19 a man in Indianapolis and she directed bank deposits to be made into Bailey's account.
20 Bailey was then directed to deposit money to various names, account numbers, and
21 routing numbers at various banks.

22 24. Bailey provided consent to search and seize evidence from his computer
23 and mobile phone. Those items were searched and found to contain communications with
24 the individuals Bailey identified as his girlfriends. Bailey received deposits into his CCU
25 bank accounts, and in those communications, it confirmed that these individuals directed
26 Bailey to withdraw money and send it to various names, account numbers, and routing
27 numbers. The girlfriends also provided specific names and addresses of people in Indiana
28 to whom Bailey mailed money.

25. Through the communications found on Bailey's computer and phone, investigators were able to directly identify phone numbers, bank accounts, and email addresses – many are the SUBJECT ACCOUNTS. Other SUBJECT ACCOUNTS were found through investigative work related to requests to Google, ESD database, Accurant, and bank information provided by Chase, Wells Fargo, PNC, and Fifth Third Bank.

26. SUBJECT ACCOUNTS on Bailey's phone and computer of individuals purporting to be Bailey's girlfriends include the following: lordchoosen7878[[@](mailto:lordchoosen7878@gmail.com)]gmail.com, lordchoosen5858[[@](mailto:lordchoosen5858@gmail.com)]gmail.com, rowenacole091[[@](mailto:rowenacole091@gmail.com)]gmail.com, jkyra924[[@](mailto:jkyra924@gmail.com)]gmail.com, noloveinthestreet[[@](mailto:noloveinthestreet@gmail.com)]gmail.com, sandrasmith88770[[@](mailto:sandrasmith88770@gmail.com)]gmail.com, and mshay743[[@](mailto:mshay743@gmail.com)]gmail.com.

27. SUBJECT ACCOUNTS of account recovery emails for the SUBJECT ACCOUNTS listed above, provided by Google in response to Section 2703(d) orders, include the following: shawngeorge122[[@](mailto:shawngeorge122@gmail.com)]gmail.com, and ryanparker12244[[@](mailto:ryanparker12244@gmail.com)]gmail.com.

28. SUBJECT ACCOUNTS of individuals who received funds from Bailey—which investigators, starting from identifying information Bailey had been provided, found through Accurant or bank information, include the following:

ppnyameengu[[@](mailto:ppnyameengu@gmail.com)]gmail.com, marbobo33[[@](mailto:marbobo33@gmail.com)]gmail.com, kamaldeenkaraole[[@](mailto:kamaldeenkaraole@gmail.com)]gmail.com, samsonnse1[[@](mailto:samsonnse1@gmail.com)]gmail.com, thompson.nse[[@](mailto:thompson.nse@gmail.com)]gmail.com, and derrykld88[[@](mailto:derrykld88@gmail.com)]gmail.com.

29. SUBJECT ACCOUNTS identified from the ESD database that requested (but may not have received) unemployment funds intended for Bailey— or were associated with Bailey and his handlers – include the following: stevestonerline[[@](mailto:stevestonerline@gmail.com)]gmail.com, pax4one10[[@](mailto:pax4one10@gmail.com)]gmail.com, lovret32[[@](mailto:lovret32@gmail.com)]gmail.com, and lovgtyr543[[@](mailto:lovgtyr543@gmail.com)]gmail.com.

30. **Walter Bailey Check Fraud Scheme:** Bailey is also involved in a check fraud scheme. Bailey receives emails from two purported individuals, James Lynn and David, that contain PDF's of checks to print. Bailey also receives from the same

1 individuals, pre-paid USPS and UPS shipping labels. The checks are drawn on victim
2 accounts and have the payee and remitters information already completed. Bailey would
3 print these checks on check stock paper and drop each package—which each contained
4 only one check—in the mail. SUBJECT ACCOUNTS from the check fraud scheme
5 include: lynnj0044[*@*]gmail.com and lamountaindave[*@*]gmail.com.

6 31. **ESD Fraud Proceeds Paid to Diana Atwood:** An additional romance
7 scheme victim, Diana Atwood (Atwood), of Oregon City, Oregon, received
8 approximately \$50,000.00 of ESD funds deposited into her bank account. She remitted
9 these ESD funds and her life savings of \$122,000.00 to an individual who identified
10 himself as “Michael Aaron” (Aaron) who purported to be from South Africa.

11 32. A few weeks into the relationship, Aaron asked Atwood to access his
12 purported bank account at Savoy Bank in New York City, New York, which is titled to
13 Bradford Enterprises (a real business). Aaron claimed he had issues accessing his bank
14 account from South Africa. Aaron provided to Atwood, over the phone, the credentials to
15 access the bank account. Atwood accessed the Bradford Enterprises bank account and an
16 automated teller provided her with the account balance of \$45,250,050.98 and indicated a
17 deposit on January 6, 2020 was on hold.

18 33. Aaron told Atwood that he needed to pay \$1,200,000.00 in taxes and fees to
19 South Africa related to his construction company, and that paying the fees would release
20 the hold on his account. Aaron asked Atwood for funds to use to pay the purported fees.
21 Between January 1, 2020 and April 28, 2020, Atwood sent Aaron funds using the Cash
22 App to two Cash App wallets in the amounts of \$28,500.00 and \$6,000.00. Atwood also
23 mailed her debit card to a Michael Aaron at Unit 20 Parklands Main Rd., Parklands
24 Milnerton, 7441, ZA (South Africa). Between March 18, 2020 through March 26, 2020,
25 there were 13 ATM withdrawals in Cape Town, South Africa, totaling \$4,110.89.

26 34. Beginning on or about April 22, 2020, Aaron asked Atwood to send him
27 Bitcoin. Aaron directed Atwood to create an account on Blockchain.com, and Atwood
28 also installed the Blockchain Wallet application on her mobile device. Atwood withdrew

1 cash funds from her personal bank accounts and retirement accounts and deposited the
2 cash funds into Bitcoin kiosks located in her local area in exchange for Bitcoin. Atwood
3 also exchanged cash for Bitcoin using a local exchanger facilitated by Aaron. Atwood
4 also used the Cash App to send Bitcoin to Aaron. Aaron provided to Atwood, via text
5 messages, the addresses to which to send Bitcoin. Atwood continued sending Bitcoin to
6 Aaron until she exhausted the funds from her savings and retirement accounts.

7 35. Atwood made these deposits into Aaron's cryptocurrency Bitcoin wallet
8 which were then transferred to wallets for Aaron's use at Luno Pte. Ltd. (Luno), a
9 cryptocurrency exchange in Singapore. Additionally, tracing those transactions led to the
10 identification of 259 total transactions related to the same Luno customer, totaling
11 \$667,669.94 from 2019 to September 2020, including \$467,561.25 in 2020.

12 36. Aaron also communicated early in the relationship with Atwood using
13 email address michaelaaron171960[*@*]gmail.com. Google subscriber records indicate
14 that the email address michaelaaron171960[*@*]gmail.com was established on or about
15 September 9, 2019, from an Internet Protocol (IP) address in South Africa and continued
16 to have logins from South Africa based IP address through June 2020. The Google
17 recovery e-mail address for michaelaaron171960[*@*]gmail.com is
18 andersondoughlas12000[*@*]gmail.com, which has a recovery SMS phone number as
19 +27619624464, which is listed with a South Africa country code. Both emails are
20 SUBJECT ACCOUNTS.

21 37. U.S. authorities are seeking records from Luno in Singapore, using a treaty
22 (MLAT), regarding the Bitcoin that was transferred from the Bitcoin wallet where
23 Atwood made deposits on behalf of Aaron. These records will assist in tracing the
24 movement and disposition of the funds sent to Luno and identifying Aaron.

25 38. **ESD Fraud Proceeds Paid to Kellie Sigurdson:** An additional romance
26 scheme victim is Kellie Sigurdson (Sigurdson), of Aurora, Illinois. Sigurdson received
27 approximately \$9,130.00 from ESD and \$9,688.00 from Massachusetts Unemployment
28 Fund. Sigurdson then sent approximately \$10,000.00 to Atwood. Sigurdson was

1 interviewed by agents and questioned on the bank transfers. She explained that she met a
2 man on a dating website purporting to be “John Maxwell” (Maxwell) and began a
3 relationship. Most of their communication was over text, where he eventually directed
4 Sigurdson to open bank accounts and a business bank account to receive deposits for
5 Maxwell. Sigurdson made the required transfers and withdrawals and communicated to
6 him via text message. The related SUBJECT ACCOUNTS are Sigurdson’s email of
7 kellielvselvis[@]gmail.com, and the email of an ESD claimant who had \$9,130.00
8 deposited into the Chase account belonging to Sigurdson: kingkorons3[@]gmail.com.

9 **BACKGROUND REGARDING EMAIL SERVICE PROVIDERS**

10 39. In my training and experience, I have learned that Google provides a
11 variety of on-line services, including electronic mail (“email”) access, to the general
12 public. Google provides subscribers email and chat accounts at the domain name
13 “[@]gmail.com.”

14 40. Subscribers obtain an account by registering with Google. When doing so,
15 Google asks the subscriber to provide certain personal identifying information. This
16 information can include the subscriber’s full name, physical address, telephone numbers
17 and other identifiers, alternative email addresses, and, for paying subscribers, means and
18 source of payment (including any credit or bank account number). In my training and
19 experience, such information may constitute evidence of the crimes under investigation
20 because the information can be used to identify the account’s user or users, and to help
21 establish who has dominion and control over the account.

22 41. Google typically retains certain transactional information about the creation
23 and use of each account on their systems. This information can include the date on which
24 the account was created, the length of service, records of log-in (i.e., session) times and
25 durations, the types of service utilized, the status of the account (including whether the
26 account is inactive or closed), the methods used to connect to the account, and other log
27 files that reflect usage of the account. In addition, email providers often have records of
28 the Internet Protocol address (“IP address”) used to register the account and the IP

1 addresses associated with particular logins to the account. As with subscriber records, IP
2 address information can help to identify which computers or other devices were used to
3 access the email account, which in turn can be used to identify the account's user or
4 users, and to help establish who has dominion and control over the account.

5 42. In some cases, email account users will communicate directly with an email
6 service provider about issues relating to the account, such as technical problems, billing
7 inquiries, or complaints from other users. Email providers typically retain records about
8 such communications, including records of contacts between the user and the provider's
9 support services, as well records of any actions taken by the provider or user as a result of
10 the communications. In my training and experience, such information may constitute
11 evidence of the crimes under investigation, because the information can be used to
12 identify the account's user or users.

13 43. In general, an email that is sent to a subscriber is stored in the subscriber's
14 "mailbox" on the email provider's servers until the subscriber deletes the email. When
15 the subscriber sends an email, it is initiated at the user's computer, transferred via the
16 Internet to the provider's servers, and then transmitted to its end destination. The email
17 provider often maintains a copy of received and sent emails. Unless the sender
18 specifically deletes an email from the email provider's server, the email can remain on
19 the system indefinitely. Even if the subscriber deletes the email, it may continue to be
20 available on the email provider's servers for some period of time.

21 44. A sent or received email typically includes the content of the message,
22 source and destination addresses, the date and time at which the email was sent, and the
23 size and length of the email. If an email user writes a draft message but does not send it,
24 that message may also be saved by the email provider but may not include all of these
25 categories of data.

26 45. In addition to email and chat, Google offers subscribers numerous other
27 services including, (i) Location History, which saves information about the physical
28 locations of devices logged into a Google account; and (ii) Web & Activity, which saves

1 information about Google web searches and browsing activity conducted by a user
2 logged into a particular Google account.

3 46. Based upon my training and experience, such information set out in the
4 preceding paragraph may be evidence of the crimes under investigation in this case. As
5 mentioned above, over the course of the investigation, law enforcement has learned that
6 an applicant can only receive for ESD benefits by providing provide an email address and
7 then logging onto that email account and activate an ESD link. The perpetrator(s) of the
8 scheme under investigation therefore must have accessed the SUBJECT ACCOUNTS in
9 the course of executing the scheme. Evidence about the location of the user of the
10 SUBJECT ACCOUNTS, as well as his/her web searches, internet activity (if such
11 information is available), and stored data in cloud-storage accounts will therefore serve as
12 evidence of the true identity of the user of the SUBJECT ACCOUNTS.

13 47. I also know that Google is also able to provide information that will assist
14 law enforcement in identifying other accounts associated with the SUBJECT
15 ACCOUNTS, namely, information identifying and relating to other accounts used by the
16 same subscriber. This information includes any forwarding or fetching accounts¹ relating
17 to the SUBJECT ACCOUNTS, all other accounts linked to the SUBJECT ACCOUNTS
18 because they were accessed from the same computer (referred to as “cookie overlap”), all
19 other accounts that list the same SMS phone number as the SUBJECT ACCOUNTS, all
20 other accounts that list the same recovery email addresses² as do the SUBJECT
21 ACCOUNTS, and all other accounts that share the same creation IP address as the
22 SUBJECT ACCOUNTS. Information associated with these associated accounts will
23
24

25
26 ¹ A forwarding or fetching account related to the SUBJECT ACCOUNT would be a separate email account that can
be setup by the user to receive copies of all of the email sent to the account.

27 ² The recovery email address is an additional email address supplied by the user that is used by the email provider to
28 confirm a username after an email account’s creation, help the user if the user is having trouble signing into their
account, or alert the user to any unusual activity involving the user’s email address.

1 assist law enforcement in determining who controls the SUBJECT ACCOUNTS and will
2 also help to identify other email accounts and individuals relevant to the investigation.

3 **REQUEST FOR NONDISCLOSURE AND SEALING**

4 48. The government requests, pursuant to the preclusion of notice provisions of
5 Title 18, United States Code, Section 2705(b), that Google be ordered not to notify any
6 person (including the subscriber or customer to which the materials relate) of the
7 existence of these warrants for such period as the Court deems appropriate. In this case,
8 such an order is appropriate because the search warrants relate to an ongoing criminal
9 investigation and disclosure would provide the targets with information about the
10 government's investigation that could be used to frustrate further investigative efforts.

11 49. I further request that the Court order that all papers in support of this
12 application, including the affidavit and search warrant, be sealed until further order of the
13 Court. These documents discuss an ongoing criminal investigation that is neither public
14 nor known to all of the targets of the investigation. There is good cause to seal these
15 documents because their premature disclosure may give the subjects an opportunity to
16 flee from prosecution, dissipate assets, destroy or tamper with evidence, change patterns
17 of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

18 50. For these reasons, I am requesting that the Court issue an order sealing the
19 search warrant, search warrant return, application and affidavit for the search warrant,
20 and all attachments for a period of 60 days.

21 **CONCLUSION**

22 51. Based on the foregoing, I believe there is probable cause to believe that
23 evidence, instrumentalities, contraband, and/or fruits of violations of Title 18, United
24 States Code, Sections 1343 and 1349 (Wire Fraud), 1956 (Money Laundering), 1957
25 (Money Laundering), and 1028A (Aggravated Identity Theft) will be found in the
26 SUBJECT ACCOUNTS, as more fully described in Attachment A to this Affidavit. I
27 therefore request that the Court issue warrants authorizing a search of the SUBJECT
28

1 ACCOUNTS, for the items more fully described in Attachment B hereto, incorporated
2 herein by reference, and the seizure of any such items found therein.

3 52. Because the warrant will be served on Google, which will then compile the
4 requested records at a time convenient to them, reasonable cause exists to permit the
5 execution of the requested warrants at any time in the day or night.

6
7
8 

9 ERIC LITSTER
10 Special Agent
11 Internal Revenue Service – Criminal Investigation

12 The above-named agent provided a sworn statement to the truth of the foregoing
13 affidavit by telephone on April 9, 2021.

14
15 

16 MARY ALICE THEILER
17 United States Magistrate Judge
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT A**Property to Be Searched**

This warrant applies to the electronically stored data, information and communications contained in, related to, and associated with, including all preserved data, the following accounts:

1. lordchoosen7878[@]gmail.com
2. lordchoosen5858[@]gmail.com
3. rowenacole091[@]gmail.com
4. jkyra924[@]gmail.com
5. noloveinthestreet[@]gmail.com
6. sandrasmith88770[@]gmail.com
7. mshay743@gmail.com
8. shawngeorge122@gmail.com
9. ryanparker12244[@]gmail.com
10. ppnyameengu[@]gmail.com
11. marbobo33[@]gmail.com
12. kamaldeenkaraole[@]gmail.com
13. samsonnse1[@]gmail.com
14. thompson.nse[@]gmail.com
15. derrykld88[@]gmail.com
16. stevestonerline[@]gmail.com
17. pax4one10[@]gmail.com
18. lovret32[@]gmail.com
19. lovgtyr543[@]gmail.com
20. lynnj0044[@]gmail.com
21. lamountaindave[@]gmail.com
22. michaelaaron171960[@]gmail.com

23. andersondoughlas12000[[@](#)]gmail.com

24. kelliuvselvis[[@](#)]gmail.com

25. kingkorons3[[@](#)]gmail.com

as well as all other subscriber and log records associated with SUBJECT ACCOUNTS, which is located at premises owned, maintained, controlled or operated by Google LLC (“Google”), an email and service provider that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California. Brackets have been placed in the name of SUBJECT ACCOUNTS to ensure that they are not inadvertently hyperlinked and contacted.

ATTACHMENT B**Particular Things to be Seized****I. Information to be disclosed by Google LLC (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each of the accounts identified in Attachment A:

a. The contents of all emails associated with the **SUBJECT ACCOUNTS**, including stored or preserved copies of emails sent to and from the accounts, draft emails, the source and destination addresses associated with each emails, the date and time at which each email was sent, and the size and length of each email;

b. All subscriber records associated with the specified accounts, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

c. All records or other information stored by any individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, and files;

1 d. any Google Chat/Messenger information and/or records, including
 2 any contact or friend list, time, date, and IP address logs for Chat and Messenger use, and
 3 any archived web messenger communications stored on servers;

4 e. any Google Search Console content from inception to the present;

5 f. any Google Web & Activity content from inception to the present;

6 g. any Google Chrome Sync content from inception to the present;

7 h. any Google Location History content from inception to the present;

8 i. any account history, including any records of communications

9 between Google and any other person about issues relating to the accounts, such as

10 technical problems, billing inquiries, or complaints from other users about the specified

11 account. This to include records of contacts between the subscriber and the provider's

12 support services, as well as records of any actions taken by the provider or subscriber in

13 connection with the service.

14 j. All records pertaining to communications between the Provider and

15 any person regarding the account, including contacts with support services and records of

16 actions taken.

17 This Search Warrant also requires Google to produce the following information

18 for SUBJECT ACCOUNTS:

19 a. list of all other accounts linked to the SUBJECT ACCOUNTS because of
 20 cookie overlap;

21 b. a list of all other accounts that list the same SMS phone number as the
 22 SUBJECT ACCOUNTS;

23 c. a list of all other accounts that list the same recovery email address as the
 24 SUBJECT ACCOUNTS; and

25 d. a list of all other accounts that shared the same creation IP address as the
 26 SUBJECT ACCOUNTS within 30 days of creation;

27 e. The Accounts referred to in subparagraphs (a) through (d) above are
 28 referred to herein as the "Linked Subject Accounts." Google shall produce

1 subscriber records for each of the Linked Subject Accounts including 1)
2 names, email addresses, and screen names; 2) physical addresses; 3)
3 records of session times and durations; 4) length of service (including start
4 date) and types of services utilized; 5) telephone or instrument number or
5 other subscriber number or identity, including any temporarily assigned
6 network address such as internet protocol address, media access card
7 addresses, or any other unique device identifiers recorded by Google in
8 relation to the account; 6) account log files (login IP address, account
9 activation IP address, and IP address history); 7) detailed billing
10 records/logs; 8) means and source of payment; and 9) lists of all related
11 accounts.

- 12 f. All records and other information (not including the contents of
13 communications) relating to the Linked Subject Accounts, including:
- 14 i. Records of user activity for each connection made to or from the
15 Linked Subject Accounts from January 1, 2020 to the present,
16 including log files; messaging logs; the date time, length, and
17 method of connections, data transfer volume; user names; and source
18 and destination Internet Protocol Addresses; cookie IDs; browser
19 type;
 - 20 ii. Information about each communication sent or received by the
21 Linked Subject Accounts from January 1, 2020 to the present,
22 including the date and time of the communication, the method of
23 communication, and the source and destination of the
24 communication (such as source and destination email addresses, IP
25 addresses, and telephone numbers);
 - 26 iii. All records pertaining to devices associated with the accounts to
27 include serial numbers, model type/number, IMEI, phone numbers,
28 MAC Addresses.

1 The Provider is hereby ordered to disclose the above information to the
2 government within 14 days of service of this warrant.

3 **II. Information to be seized by the government**

4 Upon receipt of the information described in Section I, the government shall
5 review the production and may seize the following material:

6 The following information that constitutes evidence and instrumentalities of
7 violations of Title 18 United States Code, Sections 1343 (wire fraud), 1956 (money
8 laundering), 641(theft of public funds), 371 (conspiracy); and 1028A (aggravated identity
9 theft) for the SUBJECT ACCOUNTS and any Linked Subject Accounts:

- 10 a. Content referring or relating to unemployment benefits;
- 11 b. Content referring or relating to financial transactions;
- 12 c. Content evidencing the times and methods by which the SUBJECT
13 ACCOUNTS were accessed;
- 14 d. Content that serves to identify any person who uses or accesses or
15 who exercises in any way any dominion or control over the SUBJECT ACCOUNTS;
- 16 e. Content that serves to identify any persons connected to any person
17 who accesses or who exercises in any way any dominion or control over the SUBJECT
18 ACCOUNTS; and
- 19 f. Content that serves to identify any other accounts related to the
20 SUBJECT ACCOUNTS; including accounts that share common recovery information or
21 that are linked by cookies or in any other way.
- 22 g. Content that may reveal the current or past location of the individual
23 or individuals using the account;
- 24 h. Content that may reveal the identities of and relationships between
25 co-conspirators;
- 26 i. Content that may identify any alias names, online user names,
27 “handles” and/or “nics” of those who exercise in any way any dominion or control over
28 the accounts as well as records or information that may reveal the true identities of these
individuals;
- j. Other log records, including IP address captures, associated with the
account;

1 k. Subscriber records associated with the accounts, including 1) names,
2 email addresses, and screen names; 2) physical addresses; 3) records of session times and
3 durations; 4) length of service (including start date) and types of services utilized; 5)
4 telephone or instrument number or other subscriber number or identity, Including any
5 temporarily assigned network address such as internet protocol address, media access
6 card addresses, or any other unique device identifiers recorded by Google in relation to
7 the account; 6) account log files (login IP address, account activation IP addresses, and IP
8 address history); 7) detailed billing records/logs; 8) means and source of payment; and 9)
9 lists of all related accounts;

10 l. Records of communications between Google and any person
11 purporting to be the account holder about issues relating to the account, such as technical
12 problems, billing inquiries, or complaints from other users about the specified account.
13 This to include records of contacts between the subscriber and the provider's support
14 services, as well as records of any actions taken by the provider or subscriber as a result
15 of the communications.

16 m. Android or Apple identification number, MEID, and cellular
17 telephone number

18 n. Information identifying accounts that are linked or associated with
19 the account.